In the United States Patent and Trademark Office
Board of Patent Appeals and Interferences

Appeal Brief

In re the Application of:

Glen A. Jaquette
Serial No. 09/977,159
Filed: October 11, 2001
Attorney Docket No. TUC9001022US1

METHOD, SYSTEM, AND PROGRAM FOR SECURELY PROVIDING KEYS TO ENCODE AND DECODE DATA IN A STORAGE CARTRIDGE

Submitted by:

Konrad, Raynes & Victor LLP
315 So. Beverly Dr., Ste. 210
Beverly Hills CA 90212
(310) 556-7983
(310) 556-7984 (fax)

TABLE OF CONTENTS

I. Real Party in Interest

The entire right, title and interest in this patent application is assigned to real party in interest International Business Machines Corporation.

II. Related Appeals, Interferences, and Judicial Proceedings

Appellant, Appellant's legal representative, and Assignee are not aware of any other prior or pending appeals, interferences, and judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board’s decision in the pending appeal.

III. Status of the Claims

Claims 1, 3-5, 7-16, and 44-75 are pending and have been rejected.

The fourth final office action dated June 24, 2009 ("FOA4") of the claims is being appealed for all pending claims 1, 3-5, 7-16, and 44-75.

Claims 2, 6, and 17-43 are canceled.

IV. Status of Amendments

No amendment to the claims was filed after receipt of FOA4.

V. Summary of the Claimed Subject Matter

A. Independent Claim 1

The preamble of independent claim 1 recites a method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices. The preamble is disclosed in FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and interface device 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

providing an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge

With respect to this limitation, the Specification (para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge. The Specification further discloses (para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that a single MRU key may be used for multiple storage cartridges 506a, b...n

encrypting the coding keys and storing the encrypted coding keys in the storage cartridges

With respect to this limitation, the Specification discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key

(K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I).

> receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges

With respect to this limitation, the Specification discloses that controller 518 in the interface device 502 (FIG. 11) receives an I/O request for a target storage cartridge. (Para. [0050], FIG. 13, block 610).

> mounting, by the receiving interface device, the target storage cartridge in response to the I/O request;

With respect to this limitation, the Specification discloses that the controller 518 mounts the target storage cartridge. (Para. 50, FIG. 13, block 612)

> reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge;

With respect to this limitation, the Specification discloses that the controller 518 reads the encrypted $(MRU)^H$ key from the target storage cartridge. (Para. 50, FIG. 13, block 614)

> transmitting, by the receiving interface device, the read encrypted coding key to a host device;

With respect to this limitation, the Specification discloses the controller 518 transmits the encrypted $(MRU)^H$ key 528 back to the host 500. (Para. 50, transmission shown as arrow between blocks 614 and 620)

> receiving, by the receiving interface device, the coding key encrypted by the host;

With respect to this limitation, the Specification discloses that the interface device 502 receives the encrypted coding key (MRU Key)^I. (Para. 50, receipt shown as arrow between blocks 622 and 630)

decrypting, by the receiving interface device, the coding key encrypted by the host to use for the I/O request

With respect to this limitation, the Specification discloses that the interface device 502 decrypts the encrypted MRU Key (MRU Key)^I, which the host encrypted at block 622 with the interface device public key 512 (K_I). (Paras. 50-51, block 630)

using, by the receiving interface device, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632)

using, by the receiving interface device, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632)

B. Independent Claim 10

The preamble of independent claim 10 recites a method performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device. The preamble is disclosed in FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and interface device 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

receiving an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge

With respect to this limitation, the Specification discloses that controller 770 receives the encrypted MRU key and I/O request. (Para. [0057], FIG. 15, block 770; para. [0062], FIG. 17, block 860)

mounting the storage cartridge in response to the I/O request;

With respect to this limitation, the Specification discloses that controller 770 in response to the I/O request, mounts the target storage cartridge. (Para. [0057] , block 770, FIG. 15; para. [0062], FIG. 17, block 862)

decrypting the encrypted coding key

With respect to this limitation, the Specification discloses that the controller 718 decrypts the encrypted host private key $(J_H)^I$ 726 with the interface private key J^I in the memory 722 and then use the host private key J_H 730 to decrypt (at block 776) the encrypted $(\text{MRU Key})^H$ 724 in memory to produce the MRU key 710 to use to encrypt and/or decrypt data. (Para. [0057] , block 776, FIG. 15; para. [0062], FIG. 17, block 864)

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866)

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866)

storing the received encrypted coding key in the storage medium to use for subsequent I/O requests

With respect to this limitation, the Specification discloses that upon receiving the encrypted (MRU Key)^H 724, the controller 718 may store the encrypted (MRU Key)^H 724 in the storage cartridge 506a, b...n, such as on the storage cartridge storage medium, e.g., the tape, or in a separate memory unit within the storage cartridge 506a, b...n housing, such as a cartridge memory mounted in a tape cartridge. (Para. [0058])

C. Independent Claim 47

The preamble of claim 47 recites a system for accessing data in a read/write storage medium within one of a plurality of storage cartridges and to communicate with a host. The preamble is disclosed in at least FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

an interface device having a controller for performing operations

With respect to this limitation, the Specification discloses an interface device 502. (para. 47 and FIG. 11).

> receiving an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges, wherein at least one coding key is associated with the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge, and wherein encrypted coding keys are stored in the storage cartridges

With respect to this limitation, the Specification (para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge. The Specification further discloses (para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that a single MRU key may be used for multiple storage cartridges 506a, b...n

The Specification further discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key (K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I).

The Specification further discloses that controller 518 in the interface device 502 (FIG. 11) receives an I/O request for a target storage cartridge. (Para. [0050], FIG. 13, block 610).

mounting the target storage cartridge in response to the I/O request

With respect to this limitation, the Specification discloses that the controller 518 mounts the target storage cartridge. (Para. 50, FIG. 13, block 612)

reading the encrypted coding key from the mounted target storage cartridge

With respect to this limitation, the Specification discloses that the controller 518 reads the encrypted $(MRU)^H$ key from the target storage cartridge. (Para. 50, FIG. 13, block 614)

transmitting the read encrypted coding key to a host device

With respect to this limitation, the Specification discloses the controller 518 transmits the encrypted $(MRU)^H$ key 528 back to the host 500. (Para. 50, transmission shown as arrow between blocks 614 and 620)

receiving the coding key encrypted by the host;

With respect to this limitation, the Specification discloses that the interface device 502 receives the encrypted coding key $(MRU\ Key)^I$. (Para. 50, receipt shown as arrow between blocks 622 and 630)

decrypting the coding key encrypted by the host to use for the I/O request

With respect to this limitation, the Specification discloses that the interface device 502 decrypts the encrypted MRU Key $(MRU\ Key)^I$, which the host encrypted at block 622 with the interface device public key 512 (K_I). (Paras. 50-51, block 630)

using the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632) using the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632)

D. Independent Claim 54

The preamble recites system for accessing data in a removable storage cartridge including a read/write storage medium and in communication with a host system. ,
The preamble is disclosed in at least FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

an interface device having a controller for performing operations

With respect to this limitation, the Specification discloses an interface device 802. (paras. 59-60 and FIG. 16).

receiving an encrypted coding key from the host system with an Input/Output (I/O) request directed to the storage cartridge

With respect to this limitation, the Specification discloses that controller 770 receives the encrypted MRU key and I/O request. (Para. [0057], FIG. 15, block 770; para. [0062], FIG. 17, block 860)

mounting the storage cartridge in response to the I/O request;

With respect to this limitation, the Specification discloses that controller 770 in response to the I/O request, mounts the target storage cartridge. (Para. [0057] , block 770, FIG. 15; para. [0062], FIG. 17, block 862)

decrypting the encrypted coding key

With respect to this limitation, the Specification discloses that the controller 718 decrypts the encrypted host private key $(J_H)^I$ 726 with the interface private key J^I in the memory 722 and then use the host private key J_H 730 to decrypt (at block 776) the encrypted (MRU Key)^H 724 in memory to produce the MRU key 710 to use to encrypt and/or decrypt data. (Para. [0057] , block 776, FIG. 15; para. [0062], FIG. 17, block 864)

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866)

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866) storing the received encrypted coding key in the storage medium to use for subsequent I/O requests

With respect to this limitation, the Specification discloses that upon receiving the encrypted (MRU Key)^H 724, the controller 718 may store the encrypted (MRU Key)^H 724 in the storage cartridge 506a, b...n, such as on the storage cartridge storage medium, e.g., the tape, or in a separate memory unit within the storage cartridge 506a, b...n housing, such as a cartridge memory mounted in a tape cartridge. (Para. [0058])

E. Independent Claim 61

The preamble recites an article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices. The preamble is disclosed in at least FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge. The Specification discloses (para. [0069], pg. 27) that an "article of manufacture" refers to code or logic in which the embodiments are implemented.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

providing, by the I/O manager, an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge

With respect to this limitation, the Specification (para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge.

The Specification further discloses (para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that a single MRU key may be used for multiple storage cartridges 506a, b...n The host I/O manager 516 handles I/O requests and encryption and keys. (paras. 47-49)

encrypting, by the I/O manager, the coding keys and storing the encrypted coding keys in the storage cartridges

With respect to this limitation, the Specification discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key (K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I).

receiving, by the controller, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges

With respect to this limitation, the Specification discloses that controller 518 in the interface device 502 (FIG. 11) receives an I/O request for a target storage cartridge. (Para. [0050], FIG. 13, block 610).

mounting, by the controller, the target storage cartridge in response to the I/O request;

With respect to this limitation, the Specification discloses that the controller 518 mounts the target storage cartridge. (Para. 50, FIG. 13, block 612)

reading, by the controller, the encrypted coding key from the mounted target storage cartridge;

With respect to this limitation, the Specification discloses that the controller 518 reads the encrypted $(MRU)^H$ key from the target storage cartridge. (Para. 50, FIG. 13, block 614) transmitting, by the controller, the read encrypted coding key to a host device;

With respect to this limitation, the Specification discloses the controller 518 transmits the encrypted $(MRU)^H$ key 528 back to the host 500. (Para. 50, transmission shown as arrow between blocks 614 and 620)

receiving, by the controller, the coding key encrypted by the host;

With respect to this limitation, the Specification discloses that the interface device 502 receives the encrypted coding key $(MRU\ Key)^I$. (Para. 50, receipt shown as arrow between blocks 622 and 630)

decrypting, by the controller, the coding key encrypted by the host to use for the I/O request

With respect to this limitation, the Specification discloses that the interface device 502 decrypts the encrypted MRU Key $(MRU\ Key)^I$, which the host encrypted at block 622 with the interface device public key 512 (K_I). (Paras. 50-51, block 630)

using, by the controller, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632)

using, by the controller, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the interface device 502 uses the MRU key 510 to encode/decode the data to perform the I/O request to the target storage cartridge. (Para. [0051], FIG. 13, block 632)

F. Independent Claim 68

The preamble recites an article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices. The preamble is disclosed in at least FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge. The Specification discloses (para. [0069], pg. 27) that an "article of manufacture" refers to code or logic in which the embodiments are implemented.

Below is an explanation of the claimed subject matter of claim 1 referring to the specification and drawings, where the claim limitations are underlined:

r<u>eceiving, by the controller, an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge</u>

With respect to this limitation, the Specification discloses that controller 770 receives the encrypted MRU key and I/O request. (Para. [0057], FIG. 15, block 770; para. [0062], FIG. 17, block 860)

<u>mounting, by the controller, the storage cartridge in response to the I/O request;</u>

With respect to this limitation, the Specification discloses that controller 770 in response to the I/O request, mounts the target storage cartridge. (Para. [0057] , block 770, FIG. 15; para. [0062], FIG. 17, block 862) decrypting, by the controller, the encrypted coding key

With respect to this limitation, the Specification discloses that the controller 718 decrypts the encrypted host private key $(J_H)^I$ 726 with the interface private key J^I in the memory 722 and then use the host private key J_H 730 to decrypt (at block 776) the encrypted $(\text{MRU Key})^H$ 724 in memory to produce the MRU key 710 to use to encrypt and/or decrypt data. (Para. [0057] , block 776, FIG. 15; para. [0062], FIG. 17, block 864)

using, by the controller, the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866)

using, by the controller, the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request

With respect to this limitation, the Specification discloses that the controller 718 uses (at block 778) the MRU key 710 to encode or decode data to be written or read with respect to the target storage cartridge 705a, b...n. (Para. [0057], FIG. 15, 778; para. [0062], FIG. 17, block 866)

storing, by the controller, the received encrypted coding key in the storage medium to use for subsequent I/O requests

With respect to this limitation, the Specification discloses that upon receiving the encrypted $(\text{MRU Key})^H$ 724, the controller 718 may store the encrypted $(\text{MRU Key})^H$ 724 in the storage cartridge 506a, b...n, such as on the storage cartridge storage medium, e.g., the tape, or in a separate memory unit within the storage cartridge 506a, b...n housing, such as a cartridge memory mounted in a tape cartridge. (Para. [0058])

VI. Grounds of Rejection to Be Reviewed on Appeal

A concise statement listing each ground of rejection presented for review is as follows:

A. Claims 1-17 and 44-46 are rejected under 35 U.S.C. §101 as directed to non-statutory subject matter.

B. Claims 1, 3, 5, 7-16, and 44-75 are rejected under 35 U.S.C. §103 as being unpatentable over Shear (U.S. Patent Pub. 2001/0042043) in view of Smythe (U.S. Patent No. 5,325,430) and Levy (U.S. Patent No. 5,748,744).

VII. Argument

A. Rejection Under 35 U.S.C. §101

The Examiner rejected claims 1-16 and 44-46 as directed to non-statutory subject matter (35 U.S.C. §101) on the grounds that the claims are not tied to a statutory class nor transform underlying subject matter to a different state. (FOA4, pg. 2).

As noted in the Patent Office "New Interim Patent Subject Matter Eligibility Examination Instructions", dated August 24, 2009, issued by Andrew Hirshfield to Examiners ("Instructions"), a method claim is directed to statutory subject matter if it is (1) tied to a particular machine or apparatus (machine implemented); or (2) particularly transform a particular article to a different state or thing, where the machine or transformation imposes a meaningful limit on the claim's scope. (Instructions, pgs. 5-6) and flow chart on pg. 11.

Applicants submit that this rejection is improper because independent claim 1 recites that the operations are performed by a receiving interface device, which comprises a particular machine. Additionally, the claims recite transformations of subject matter, in the form of encrypting the coding key, transmitting the coding key, decrypting the coding key encrypted by the host, and using the decrypted coding key to read and write data to the target storage, all of which claimed operations involve the transformation of underlying subject matter, both the coding key and the data being coded and decoded.

Applicants further submit that claim 1's use of the machine, an interface device, and transformations provide meaningful limitations on the scope of the claim because the machine and transformation claim requirements distinguish over the cited art for the reasons discussed below. Thus, the machine and transformation limitations impose actual boundaries on the scope of the claims. See, Instructions, pgs. 5-6.

Accordingly, claim 1 and claims 2-16 and 44-46 that depend therefrom are directed to patentable subject matter.

For these reasons, Applicants request that the Board reverse the Section 101 rejection.

B. Rejection Under 35 U.S.C. §103 as obvious over Shear, Smythe and Levy

1. Claims 1, 4, 5, 7, 44, 47, 49, 50, 52, 61, 63, 64, 65, and 67

With respect to claims 1, 47, and 61, Applicants request reconsideration and reversal of the Examiner's finding that col. 3, lines 40-62 of Smythe teaches the claim requirement of receiving and decrypting, by the receiving interface device, the coding key encrypted by the host to use for the I/O request. (FOA, pg. 4) The cited col. 3 mentions a microprocessor connected via an encrypted address and data bus to a RAM, and the bus is encrypted using software logic within the microprocessor. The microprocessor includes an address encryptor and data encryptor, that both depend on an encryption key.

Although the cited Smythe discusses how a microprocessor encrypts data and addresses on a bus, the cited Smythe does not teach the specific claim requirements of claims 1, 47, and 61 that an interface device receives and decrypts a coding key encrypted by a host to use for an I/O request. Instead, the cited Smythe discusses how a microprocessor has an address and data encryptors to encrypt and decrypt data. There is no discussion in the cited Smythe of an interface device receiving and decrypting a coding key encrypted by a host, where the interface device previously transmitted the encrypted coding key to the host.

Applicants request review and reversal of the Examiner's finding that col. 7, lines 63-60 of Smythe teaches the claim requirements of claims 1, 47, and 61 of using, by the receiving interface device, the decrypted coding key to decode data to read and write with respect to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request. (FOA, pg. 4). The cited col. 7 mentions an intercept routine to intercept read/write calls to disks, where the intercept routine decrypts/encrypts each sector read/written using a key.

Although the cited col. 7 discusses using a key to decrypt data, this does not teach the requirement of claims 1, 47, and 61 that the coding key used to decrypt/encrypt is itself decrypted in the claimed manner.

Applicants request review and reversal of the Examiner finding that col. 4, lines 6-12 and 53-60 of Levy teach the requirement of claims 1, 47, and 61 of encrypting the coding keys and storing the encrypted coding keys in the storage cartridges. (FOA, pg. 5)

The cited col. 4 mentions using three cryptographic keys for security, a controller key embedded within the peripheral controller during manufacture, a media key stored in mass storage device, and user supplied key 12a used by the user. Tapes and CD ROMS may also use one to three keys, where the use of three keys provides a level of enhanced security. Although the cited col. 4 of Levy discusses using multiple keys, the Examiner has not cited any part of Levy that teaches or suggests encrypting the cryptographic keys and storing encrypted coding keys in the storage cartridges. The cited col. 4 discusses storing a media key 14a on the storage device, but not encrypted keys as claimed.

Applicants request review and reversal of the Examiner finding that that col. 5, line 54 to col. 6, line 3 and col. 6, lines 33-52 of Levy teach the requirements of claims 1, 47, and 61 that the interface device read the encrypted coding key from a mounted storage cartridge, transmit the encrypted coding key to a host, and then receive the coding key encrypted by the host to decrypt and use. (FOA, pg. 5)

The cited cols. 5-6 discuss a Cipher Enable command that enables encrypted media using a hash derived from a user supplied keyphrase. The Cipher Enable command sets the media as an encrypted partition to appear to the user as a separate volume accessed with different logical unit numbers to distinguish from non-encrypted data. The cited col. 6 further mentions a command set to initialize a mass storage means to store encrypted data, allowing selection of a keyphrase during initialization of the storage, and allowing input of the keyphrase to unlock the key to access the encrypted data on the storage.

Although the cited cols. 5 and 6 of Levy discusses how to encrypt data on a storage using a user supplied keyphrase, there is no teaching of the claim requirements that the interface device read the encrypted coding key from a storage cartridge and transmit to a host, and then receive the coding key encrypted by the host, which the interface device then decrypts and uses. Instead, the cited Levy discusses how to use a user supplied keyphrase to decrypt data. The Examiner has not cited any part of Levy that teaches that that an interface device read the encrypted coding key, transmit to a host, and then receive the coding code encrypted by the host.

Accordingly, claims 1, 47, and 61 are patentable over the cited combination because the cited Shear, Smythe and Levy do not teach or suggest all the claim requirements.

For these reasons, Applicants request that the Board reverse the obviousness rejection of claims 1, 47, and 61.

Applicants submit that claims 4, 5, 7, 44, 49, 50, 52, 63, 65, and 67 are patentable over the cited art because they depend from one of claims 1, 47, and 61, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

2. Claims 3, 48, and 62

First off, Applicants submit that claims 3, 48, and 62 are patentable over the cited art because they depend from one of claims 1, 47, and 61, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, with respect to claims 3, 48, and 62, Applicants request review and reversal of the Examiner's finding that FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the claim requirements that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges. (FOA, pg. 6)

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable. The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties. The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media. The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. Although the cited Shear discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches that one key is associated with a plurality of storage cartridges, wherein this one key is used to code and decode data from the storage mediums of the storage cartridges.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 3, 48, and 62.

For these reasons, Applicants request the Board to reverse the rejection of claims 3, 48, and 62.

3. Claims 8, 51, and 66

First off, Applicants submit that claims 8, 51, and 66 are patentable over the cited art because they depend from one of claims 1, 47, and 61, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, with respect to claims 8, 51, and 66, Applicants request review of the Examiner's findings that FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the claim requirement encrypting the coding key comprising encrypting, by the host (or I/O manager in the case of claim 65), the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key. (FOA, pg. 7)

As discussed, the above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Shear discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the coding key with a first key, where the host uses a second key to decrypt the coding key, and that the host encrypts the coding key with a third key, and that the interface device, or cited drive, uses a fourth key the key that is then used to decrypt the coding key, or cited encrypted key block.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 8, 51, and 66.

For these reasons, Applicants request the Board to reverse the rejection of claims 8, 51, and 66.

4. Claims 45 and 53

First off, Applicants submit that claims 45 and 53 are patentable over the cited art because they depend from base claims 1 and 47, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, claims 45 and 53 depend from claims 8 and 51, respectively, and further require that the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

The Examiner cited the same art as cited against claim 17, including the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear. (FOA4, pg. 11)

As discussed, the above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

However, the Examiner has not specifically cited any claim requirement that the coding key on the disk of Shear is encrypted with a host public key and that a host uses a host private key to decrypt the coding key, and that a host encrypts the decrypted coding key with an interface device public key as claimed. Instead, the cited Shear discusses how a key is encrypted in an encrypted key block in a drive. The Examiner has not cited any part of Shear that mentions that the key on in the encryption block of Shear is sent to a host to decrypt with a host public key such that the host then encrypts with an interface device public key to return to the interface device to decrypt with an interface device private key.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 45 and 53.

For these reasons, Applicants request the Board to reverse the rejection of claims 45 and 53.

5. Claims 10, 11, 13-15, 54, 56-58, 68, 69, and 71-73

Independent claims 10, 54, and 68 recite an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, comprising: receiving an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge; mounting the storage cartridge in response to the I/O request; decrypting the encrypted coding key; using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request; using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

Applicants request review of the Examiner’s findings that the above cited paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the requirements of claims 10, 54, and 68. (FOA, pg. 8)

Applicants submit that the Examiner has not cited any part of Shear that teaches or suggests an interface device for accessing a coupled storage medium that receives an encrypted coding key from a host with an I/O request directed to the storage cartridge, mounting the storage cartridge in response to the received I/O request, decrypting the encrypted coding key, and using the coding key to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD). In the cited para. 81 and 217, the storage medium having the encrypted data carries the decryption key in a hidden portion, which is decrypted with another key, or the keys may be stored in a drive key store. This does not teach decrypting the encrypted encoding key received from a host system with an I/O request directed to the storage cartridge to use encode data to write to the storage medium in the storage cartridge for said I/O request.

Further, the Examiner has not cited any part of Shear that teaches the claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. However, these cited sections do not teach that the disk drive, which decrypted and used a key to code data to write to the storage, stores an encrypted coding key received from a host system with an I/O request in the storage medium for subsequent I/O requests.

Applicants note that the Examiner did not cite references other than Shear with respect to claims 10, 54, and 68.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 10, 54, and 68.

For these reasons, Applicants request the Board to reverse the rejection of claims 10, 54, and 68.

Applicants submit that claims 11, 13-15, 56-58, 69, and 71-73are patentable over the cited art because they depend from one of claims 10, 54, and 68, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

6. Claims 12, 55, and 70

First off, Applicants submit that claims 12, 55, and 70 are patentable over the cited art because they depend from one of claims 10, 54, and 68, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, with respect to claims 12, 55, and 70, Applicants request review of the Examiner's findings that FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the claim requirement that the coding key is encrypted by a first key maintained at the host system, further comprising maintaining, by the interface device, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key. (FOA4, pg. 9)

As discussed, the above cited Shear mentions that a drive may access an encrypted key from disk, decrypt the key using another key, and use the decrypted key do decrypt data from the disk. Although the cited Shear discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the coding key with a first key and that the interface device maintains a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 12, 55, and 70.

For these reasons, Applicants request the Board to reverse the rejection of claims 12, 55, and 70.

7. Claims 16, 59, and 74

First off, Applicants submit that claims 16, 59, and 74 are patentable over the cited art because they depend from one of claims 10, 54, and 68, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, claims 16, 59, and 74 further require that the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by: receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key.

Applicants request review and reversal of the Examiner's findings that the above discussed Shear teaches the additional claim requirements. (FOA4, pg. 10)

Applicants submit that the Examiner has not cited any part of Shear that teaches that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear discloses that the disk drive receives a further key that is used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217 mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 16, 59, and 74.

For these reasons, Applicants Accordingly, Applicants request the Board to reverse the rejection of claims 16, 59, and 74.

8. Claims 46, 60, and 75

First off, Applicants submit that claims 46, 60, and 75 are patentable over the cited art because they depend from one of claims 10, 54, and 68, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

Moreover, claims 46, 60, and 75 further require that the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

The Examiner cited the same art as cited against claim 17, including the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear. (FOA4, pg. 11) Applicants review and reversal of these finding.

As discussed, the above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The above cited Shear discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

However, the Examiner has not cited any part of Shear that teaches that the coding key on the disk of Shear is encrypted with a host public key and that a host uses a host private key to decrypt the coding key, and that a host encrypts the decrypted coding key with an interface device public key as claimed. Instead, the cited Shear discusses how a key is encrypted in an encrypted key block in a drive. The Examiner has not cited any part of Shear that mentions that the key on in the encryption block of Shear is sent to a host to decrypt with a host public key such that the host then encrypts with an interface device public key to return to the interface device to decrypt with an interface device private key.

Accordingly, the cited Shear does not teach or suggest the additional requirements of claims 46, 60, and 75.

For these reasons, Applicants request the Board to reverse the rejection of claims 46, 60, and 75.

C. Conclusion

Each of the rejections set forth in the FOA4 are improper and should be reversed.

Respectfully submitted,

/David Victor/

David W. Victor
Reg. No. 39,867

Dated: November 11, 2009

Direct All Correspondence to:
David Victor
Konrad Raynes & Victor LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, California 90212
Tel: 310-553-7977
Fax: 310-556-7984

VIII. Claims Appendix

1. (Previously Presented) A method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, comprising:

providing an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge;

encrypting the coding keys and storing the encrypted coding keys in the storage cartridges;

receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges;

mounting, by the receiving interface device, the target storage cartridge in response to the I/O request;

reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge;

transmitting, by the receiving interface device, the read encrypted coding key to a host device;

receiving, by the receiving interface device, the coding key encrypted by the host;

decrypting, by the receiving interface device, the coding key encrypted by the host to use for the I/O request;

using, by the receiving interface device, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and

using, by the receiving interface device, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

4. (Original) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

5. (Original) The method of claim 1, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

6. (Canceled)

7. (Previously Presented) The method of claim 1, wherein encrypting the coding key further comprises:

encrypting, by the host, the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

8. (Previously Presented) The method of claim 1, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by encrypting the coding key with a third key, wherein the interface devices uses a fourth key to decrypt the coding key encrypted by the host with the third key.

9. (Canceled)

10. (Previously Presented) A method performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, comprising:

receiving an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge;

mounting the storage cartridge in response to the I/O request;

decrypting the encrypted coding key;

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and

storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

11. (Previously Presented) The method of claim 10, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data is only encoded or decoded using the coding key.

12. (Previously Presented) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, further comprising;

maintaining, by the interface device, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

13. (Original) The method of claim 12, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

14. (Original) The method of claim 13, further comprising:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

15. (Original) The method of claim 12, further comprising:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

16. (Previously Presented) The method of claim 10, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by:

receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system; and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

17-43. (Canceled)

44. (Previously Presented) The method of claim 1, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

45. (New) The method of claim 8, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

46. (New) The method of claim 16, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

47. (New) A system for accessing data in a read/write storage medium within one of a plurality of storage cartridges and to communicate with a host, comprising:

an interface device having a controller for performing operations, the operations comprising:

receiving an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges, wherein at least one coding key is associated with the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge, and wherein encrypted coding keys are stored in the storage cartridges;

mounting the target storage cartridge in response to the I/O request;

reading the encrypted coding key from the mounted target storage cartridge;

transmitting the read encrypted coding key to a host device;

receiving the coding key encrypted by the host;

decrypting the coding key encrypted by the host to use for the I/O request;

using the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and using the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

48. (New) The system of claim 47, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

49. (New) The system of claim 47, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

50. (New) The system of claim 47, wherein encrypting the coding key further comprises:

encrypting, by the host, the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

51. (New) The system of claim 47, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by

encrypting the coding key with a third key, wherein the interface devices uses a fourth key to decrypt the coding key encrypted by the host with the third key.

52. (New) The system of claim 47, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

53. (New) The system of claim 51, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

54. (New) A system for accessing data in a removable storage cartridge including a read/write storage medium and in communication with a host system, comprising:

an interface device having a controller for performing operations, the operations comprising:

receiving an encrypted coding key from the host system with an Input/Output (I/O) request directed to the storage cartridge;

mounting the storage cartridge in response to the I/O request;

decrypting the encrypted coding key;

using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;

using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and

storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

55. (New) The system of claim 54, wherein the coding key is encrypted by a first key maintained at the host system, wherein the operations further comprise:

maintaining a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

56. (New) The system of claim 55, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

57. (New) The system of claim 56, wherein the operations further comprise:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

58. (New) The system of claim 55, wherein the operations further comprise:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

59. (New) The system of claim 54, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by:

receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system; and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

60. (New) The system of claim 59, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

61. (New) An article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, wherein the controller and I/O manager are executed to perform:

providing, by the I/O manager, an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge;

encrypting, by the I/O manager, the coding keys and storing the encrypted coding keys in the storage cartridges;

receiving, by the controller, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges;

mounting, by the controller, the target storage cartridge in response to the I/O request;

reading, by the controller, the encrypted coding key from the mounted target storage cartridge;

transmitting, by the controller, the read encrypted coding key to a host device;

receiving, by the controller, the coding key encrypted by the host;

decrypting, by the controller, the coding key encrypted by the host to use for the I/O request;

using, by the controller, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and

using, by the controller, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

62. (New) The article of manufacture of claim 61, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage

mediums and decode data read from the storage mediums of the plurality of storage cartridges.

63. (New) The article of manufacture of claim 61, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

64. (New) The article of manufacture of claim 61, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

65. (New) The article of manufacture of claim 61, wherein encrypting the coding key further comprises:

encrypting, by the I/O manager, the coding key with a first key, wherein the controller uses a second key to decrypt the coding key encrypted with the first key.

66. (New) The article of manufacture of claim 61, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein the host uses a second key to decrypt the coding key encrypted with the first key, wherein the host encrypts the coding key by

encrypting the coding key with a third key, wherein the controller uses a fourth key to decrypt the coding key encrypted by the host with the third key.

67. (New) The article of manufacture of claim 61, wherein the storage cartridges comprise tape media and the data on the storage cartridges coded and decoded using the at least one coding key comprises archival data.

68. (New) An article of manufacture comprising at least one of a computer readable storage media and hardware including an Input/Output (I/O Manager) and controller for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, wherein the controller and I/O manager are executed to perform:

receiving, by the controller, an encrypted coding key from the I/O manager with an Input/Output (I/O) request directed to the storage cartridge;

mounting, by the controller, the storage cartridge in response to the I/O request;

decrypting, by the controller, the encrypted coding key;

using, by the controller, the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request;

using, by the controller, the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and

storing, by the controller, the received encrypted coding key in the storage medium to use for subsequent I/O requests.

69. (New) The article of manufacture of claim 68, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data is only encoded or decoded using the coding key.

70. (New) The article of manufacture of claim 68, wherein the coding key is encrypted by a first key maintained by the I/O manager, wherein the operations further comprise:

maintaining, by the controller, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key to decrypt the coding key encrypted with the first key.

71. (New) The article of manufacture of claim 70, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

72. (New) The article of manufacture of claim 71, wherein the operations further comprise:

transmitting, by the controller, the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

73. (New) The article of manufacture of claim 70, wherein the operations further comprise:

storing, by the controller, the coding key encrypted with the first key within the storage cartridge;

receiving, by the controller, an input/output (I/O) request directed to the storage cartridge; and

accessing, by the controller, the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

74. (New) The article of manufacture of claim 68, wherein the received encrypted coding key is encrypted by a first key maintained by the I/O manager, wherein the I/O manager maintains a second key to decrypt data encrypted using the first key, wherein the controller decrypts the encrypted coding key by:

receiving, with the I/O request, from the I/O manager he second key encrypted by the I/O manager using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the I/O manager and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

75. (New) The article of manufacture of claim 74, wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

IX. Evidence Appendix

None

X. Related Proceedings Appendix

None